

TESTIMONY OF MICHAEL O'HANLON BEFORE THE HOUSE COMMITTEE
ON HOMELAND SECURITY, OCTOBER 31, 2007

A Hearing on "Enhancing and Implementing the Cybersecurity Elements of the
Sector Specific Plans"

Greetings. It is an honor to appear before the committee today.

My opening comments will be brief and rather broad. I am not an expert on cybersecurity, hence my contribution today will involve creating a framework within which this important aspect of homeland security can be considered and analyzed.

It is useful to think in terms of different possible strategies for homeland security. Clearly, in a society like ours, huge as it is, as open and free as it is, we could be far more diligent about protecting ourselves from terrorism than we are today.

For example, if the degree of terrorist threat here was anything approaching that in Israel, or if even a single additional major attack had been successfully carried out since 9/11, we would do things that are presently seen as politically infeasible or strategically unnecessary (such as searching baggage on most trains and buses, tightening up land borders far more, and worrying about truck bomb vulnerability at far more prominent buildings).

But we are already much more diligent than we were before 9/11, and are spending more than \$50 billion a year in federal funds on the effort (whereas a decade ago we spent perhaps one fifth as much on counterterrorism, and did not even employ the term homeland security in the federal lexicon). So our current strategy might be seen as an intermediate one along a spectrum of possible approaches.

A notional list of a full spectrum of possible approaches to homeland security might look something like this, in ascending order of intensity and cost:

- Pre-9/11 Approach. The philosophy here would be to protect only against very specific threats that have manifested themselves before, or that would be especially worrisome. For example, we protected nuclear power plants from sabotage, and top officials from assassination. The annual cost to the federal government is under \$10 billion for such an approach, roughly and notionally speaking.
- Post-9/11 Threat-Based Approach. This approach would follow a similar logic but expand the list of credible threats based on what we learned on September 11, 2001 and in various events around the world since then. Jeremy Shapiro of Brookings is a proponent of this approach (see opportunity08.org). Airline security is an obvious area of focus for this

approach, which would emphasize prevention of what we know that al Qaeda and related groups CAN do, as opposed to what they might wish to do. Reducing our vulnerability to truck bombs at prominent sites is another logical area of emphasis, given known patterns of terrorist activity around the world. The annual cost is about \$20 billion to \$30 billion (my estimates).

- Bush Administration Approach. This goes beyond the threat-based approach to include as well attention to those types of attacks that we know al Qaeda would LIKE to carry out, as well as those that would be so horrible we have to worry that they might occur even if they probably will not (such as WMD attacks). Estimated annual cost \$50 billion.
- Brookings Approach. This approach, reflected in two Brookings studies this decade by a team of authors, is similar in some ways to the Bush administration's concept. But it takes a slightly broader approach to defining threats and toughens up the steps taken to address them in some cases. We focus primarily on attacks that could cause major damage to our national security, our population, or our economy (catastrophic attacks). For example, we emphasize better protection of the chemical industry and the hazardous trucking industry, as well as improved use of intelligence to find patterns of possible terrorist attack before they occur (a "google function for counterterrorism") along the lines also proposed by the Markle Foundation. Estimated yearly cost \$60 billion.
- "America the Vulnerable" approach. I borrow here from Stephen Flynn of the Council on Foreign Relations; former Bush administration homeland security official Clark Kent Ervin has written a somewhat similar book. The approach here is to take imagination to its logical extreme, and suppose that any serious attack al Qaeda might be able to carry out we should defend robustly against. It is a vulnerability-based approach, but with vulnerability defined in a broad way. Great attention is paid to inspecting cargo in international shipping by Flynn, for example, even though it could be very difficult to rework our port infrastructure to make this possible. Estimated cost \$80 billion a year.
- Council on Foreign Relations task force approach. This Hart-Rudman task force of several years ago reflected the logic of Flynn, who was involved with the project as well, and also placed particular emphasis on equipping and training most of America's millions of first responders to deal with WMD attacks and other catastrophes. About \$90 billion a year.
- Israel-style approach. If we had to worry about small bombs going off in most public places, a whole different level of effort would be required, with annual costs perhaps reaching \$200 billion (and many inconveniences introduced to daily life).

This is a very short written testimony but I hope its succinctness will be of some use in providing a simple taxonomy for further discussion. I would be happy in particular to explain the Brookings approach, both in broad philosophy and in its specific recommendations.